Introduction: Cybersecurity and Software Assurance Minitrack

Luanne Chamberlain, Richard George, Thomas Llansó
Johns Hopkins Applied Physics Laboratory
11100 Johns Hopkins Road Laurel, MD 20723
Luanne.Chamberlain, Richard.George, Thomas.llanso@jhuapl.edu

The Cybersecurity and Software Assurance Minitrack is focused on improving the community's collective understanding of the scientific underpinnings of the fields of information and software security. The Minitrack's broad Call for Papers reflects the complex and multidimensional nature of these related fields. Progress cannot come soon enough, as evidence continues to accumulate documenting the significant advantage that cyber attackers maintain over cyber defenders.

The papers for this year's minitrack are representative of the diversity of the Minitrack's Call for Papers and include a new concept for a computing machine that resists sabotage by malware, an approach for continuously certifying cloud services, the introduction of a set of measures for assessing the robustness of autonomous agent collaboration, and the derivation of a controlled experiment designed to rigorously validate the effectiveness of systems security analytics.

In the first paper, *A Cryptographically Stable Computing Machine*, Michael Stephen Fiske, from AEMƎA Institute, discusses an approach for transforming a set of machine instructions in a register machine into a "stable" version that hides instruction operands and opcodes. These changes are intended to help counteract attempts by attackers to make small changes to the programs instructions (e.g., to branching addresses) that can prevent the code from becoming or referencing malware.

In the second paper, *Using ChatOps to Achieve Continuous Certification of Cloud Services*, Paul Ohagen of the HECTOR School of Management and Engineering, and Sebastian Lins, Scott Thiebes, and Ali Sunyaev from the Karlsruhe Institute of Technology, discuss the use of "ChatOps" as part of a technical solution for enabling "continuous certification" of cloud services. The solution is a monitoring-based service certification system. The paper couches the technical solution in terms of the principles of Design Science Research.

In the third paper, *Tackling Challenges of Robustness Measures for Agent Collaboration in Open Multi-Agent Systems*, by David Jin, Niclas Kannengießer, Benjamin Sturm, and Ali Sunyaev of the Karlsruhe Institute of Technology, employs thematic analysis to survey the scientific literature for robustness measures for cooperating agents. Agents are autonomous software programs that assist humans in completing various tasks. The paper focses on agents that are capable of forming ad-hoc coalitions, so-called open multi-agent systems. Such systems are capable of completing more complex tasks than single agents.

In the fourth and final paper, *Rigorous Validation of Systems Security Engineering Analytics*, by Thomas Llansó, Martha McNeil, and Jessie Jamieson of the Johns Hopkins Applied Physics Laboratory, the topic of validating systems security engineering analytics is discussed in the context of an experimental design meant to determine the degree of effectiveness of a candidate systems security analytic. This research ties to the assurance dimension of the minitrack and includes a model for estimating the cost of running such an experiment at scale.

URI: https://hdl.handle.net/10125/80250
978-0-9981331-5-7